

Received November 17, 2017, accepted December 28, 2017, date of publication January 29, 2018, date of current version March 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2799244

# Unlocking the Deployment of Spectrum Sharing With a Policy Enforcement Framework

CARLO GALIOTTO<sup>1</sup>, GEORGE K. PAPAGEORGIOU<sup>2</sup>,  
KONSTANTINOS VOULGARIS<sup>2</sup>, (Member, IEEE), M. MAJID BUTT<sup>3</sup>, (Senior Member, IEEE),  
NICOLA MARCHETTI<sup>1</sup>, AND CONSTANTINOS B. PAPADIAS<sup>2</sup>, (Fellow, IEEE)

<sup>1</sup>CONNECT Centre, Trinity College Dublin, Dublin 2, Ireland

<sup>2</sup>Broadband Wireless and Sensor Networks Laboratory, Athens Information Technology, 151 25 Athens, Greece

<sup>3</sup>Electronics and Electrical Engineering Department, University of Glasgow, Glasgow G12 8QQ, U.K.

Corresponding author: C. Galiotto (galiotc@tcd.ie)

This work was supported in part by the European Commission FP7 Research Project ADEL under Agreement 619647 and in part by a research grant from the Science Foundation Ireland and is co-funded under the European Regional Development Fund under Grant 13/RC/2077.

**ABSTRACT** Spectrum sharing has been proposed as a promising way to increase the efficiency of spectrum usage by allowing incumbent operators (IOs) to share their allocated radio resources with licensee operators (LOs), under a set of agreed rules. The goal is to maximize a common utility, such as the sum rate throughput, while maintaining the level of service required by the IOs. However, this is only guaranteed under the assumption that all “players” respect the agreed sharing rules. In this paper, we propose a comprehensive framework for licensed shared access (LSA) networks that discourages LO misbehavior. Our framework is built around three core functions: misbehavior detection via the employment of a dedicated sensing network; a penalization function; and, a behavior-driven resource allocation. To the best of our knowledge, this is the first time that these components are combined for the monitoring/policing of the spectrum under the LSA framework. Moreover, a novel simulator for LSA is provided as an open access tool, serving the purpose of testing and validating our proposed techniques via a set of extensive system-level simulations in the context of mobile network operators, where IOs and several competing LOs are considered. The results demonstrate that violation of the agreed sharing rules can lead to a great loss of resources for the misbehaving LOs, the amount of which is controlled by the system. Finally, we promote that including a policy enforcement function as part of the spectrum sharing system can be beneficial for the LSA system, since it can guarantee compliance with the spectrum sharing rules and limit the short-term benefits arising from misbehavior.

**INDEX TERMS** Spectrum sharing, licensed shared access (LSA), misbehavior detection, mobile network operators (MNO), policy enforcement framework, system-level simulator, dedicated sensing network (DSN).

## I. INTRODUCTION

The increased demand for spectrum, over the past few years, has led to research directions that were considered inconceivable a few decades ago. One of the pursued paths has led to the establishment of spectrum sharing, which was predominantly based on the concept of Cognitive Radio (CR) [1], [2]. Later, more structured sharing frameworks such as Licensed Shared Access (LSA) and Spectrum Access Sharing (SAS) have been introduced in Europe and in the United States, respectively; these are built on a central controller that assists different tiers of spectrum users to access common bands, according to some agreed policies [3]. Their major difference lies in the fact that the SAS is designed to ensure coexistence with IOs

which are not able to provide any *a priori* information to a central database, as opposed to the LSA.

Despite its promising outlook and the registered interest from a range of industrial players, spectrum sharing is still met with quite some skepticism by the National Regulatory Authorities (NRAs), holding back its deployment, especially across Europe. Among the major concerns is the lack of guarantee that spectrum users can be effectively offered interference-free and QoS-assured access to spectrum. Attempting to access the spectrum during non-granted slots would inevitably result in harmful interference and QoS performance degradation. To this day, the LSA framework, which is defined by the European Electronic

Communications Committee (ECC) report in [4], does not specify how to prevent LSA players from accessing non-granted resources and, currently, interference avoidance relies on the incumbents' and LSA licensees' commitment to fully comply with the agreed rules.

Therefore, monitoring violations and preventing misbehaving activity (either intentional or unintentional) is one of the key enablers for the adoption of spectrum sharing by NRAs, as well as the industry.

In this work, we present a novel approach for discouraging misbehavior in an LSA system,<sup>1</sup> where several LOs contend for the same resources. We specifically focus on the misbehavior of LOs trying to access LSA channels during forbidden time slots. Furthermore, we propose a detection mechanism on top of the LSA architecture that can carry out the misbehavior detection and the penalization in a centralized manner. The proposed policy enforcement framework is composed of:

- a Dedicated Sensing Network (DSN) operating in real-time according to a detection algorithm,
- a penalization function that assigns a penalty score for each LO according to its behavior,
- a resource allocation strategy that takes into account the penalty scores.

It should be noted that, to the best of our knowledge, this is the first time that these different components are unified under the context of spectrum sharing in LSA networks.

For the validation of the proposed framework, and due to the lack of a suitable tool, we have developed a system-level simulator for LSA networks that incorporates the functionality of misbehavior detection. It is implemented in Matlab and is offered as open source code in [5]. Our system-level results demonstrate that penalizing licensee misbehavior, by restricting its access to the shared resources, eradicates potential benefits from misbehaving activity. Therefore, LOs are motivated to fully comply with the agreed sharing rules.

The rest of the paper is organized as follows: First, we provide an overview of the related work in Section II. In Section III, we present the considered LSA system architecture and topology. A description of the policy enforcement approach is provided in Section IV. In Section V, we present the basic components of the LSA system-level simulator. Section VI describes our system-level results. Finally, in Section VII, we summarize our findings.

## II. RELATED WORK

Spectrum sharing is a broad area of research that has been extensively investigated, in particular after the introduction of Cognitive Radio and Dynamic Spectrum Access (DSA) concepts [6], [7], [8]. However, the proposed work for policy enforcement in spectrum sharing environments is rather limited. A classification of different approaches to policy enforcement has been presented in [9], where the authors

distinguish between two main categories. The first category includes the *ex-ante* approaches, i.e., measures that aim at preventing misbehavior (e.g., device certification or testing to ensure devices follow specific spectrum access procedures). The second category is comprised of the *ex-post* approaches, in which action is taken after the occurrence of misbehavior and implies sanctions such as restrictions to spectrum access. Our proposed policy enforcement belongs to the latter category.

Due to the wide variety of existing spectrum access schemes, each proposed solution needs to be tailored to different system requirements, such as the availability of centralized controller, the hierarchy in terms of spectrum access rights among different tiers of users, cost of implementation, etc. Among all, the solutions to spectrum policy enforcement that most closely relate to our approach are [6], [7], and [8].

In [6], Maruenda-Hernández *et al.* consider policy enforcement for dynamic spectrum leasing, where IOs dynamically change the amount of spectrum they are willing to share. This is achieved by modifying the threshold of the tolerable interference, while the LOs adjust their transmit power accordingly. The detection of potential spectrum violations is performed by the IOs via the evaluation of the cross-correlation between the IO's and the LO's signals. In case of violation detection by either the IOs or the LOs, a penalty is applied forcing the misbehaving operator to reduce its transmit power, according to the pre-agreed rules.

In [7], Kumar *et al.* consider spectrum sharing between an incumbent and a licensee operator, in the context of CR, where a third entity acts as a moderator or enforcer. The LO's activity is detected by the IO, while the moderator is in charge of enforcing the sanctions for the licensee, by restricting its spectrum access for some time. The authors model this problem as a game theoretic one and show that, by properly tuning some given parameters, i.e., the cost of violation reporting for the IO and the penalty for the LO, there is no incentive for any of the players to misbehave. In other words, the IO has no incentive to report false interference from the LO, while the LO would not receive any long-term benefits from transmitting on the band currently occupied by the incumbent. However, the study reported in [7] is limited to a game between an incumbent and a licensee operator; in our work, we deal with a more complex scenario with several players, both incumbents and licensees.

A policy enforcement approach for SAS systems has been proposed in [8], where the authors focus on the spectrum violations occurring at tier-3—Generalized Authorized Access (GAA) users—and potentially harming tier-2—Priority Access License (PAL) spectrum users. In their work, detection is carried out in a “crowdsourced” manner, i.e., is performed by a crowd of user terminals distributed in the network. The authors mainly focus on the detection task, and formulate a game-theoretical analysis of the enforcement cost, in order to reduce the number of undetected violations. The concept of penalization and its consideration for the allocation of resources is not addressed here.

<sup>1</sup>In principle, the policy enforcement framework can be applied to SAS as well. However, it is not the direction that we followed in this work.

With respect to the aforementioned related work, our paper considers LSA as the underlying spectrum sharing framework and assumes that both detection and penalization are performed by a central entity, i.e., the DSN and the LSA band manager, which are part of the LSA framework managing and controlling the spectrum. From our point of view, this seems like a natural choice, given that LSA is intrinsically centralized. Moreover, it is controlled by an impartial actor that can be trusted by all players (both IOs and LOs). The idea of integrating the penalty in the assignment of LSA spectrum to an LO was introduced in [10], where the authors also investigated the short-term and long-term behavior for different penalty functions on the LOs' throughput. However, there was no misbehavior detection and the results were based on simplified simulations. The current work represents the first attempt that addresses the policy enforcement for LSA in a comprehensive manner, which includes misbehavior detection and penalty assignment.

### III. PROPOSED LSA NETWORK

In the current section, we describe the components of our proposed network architecture, which is an extension of the original LSA framework defined in [4].

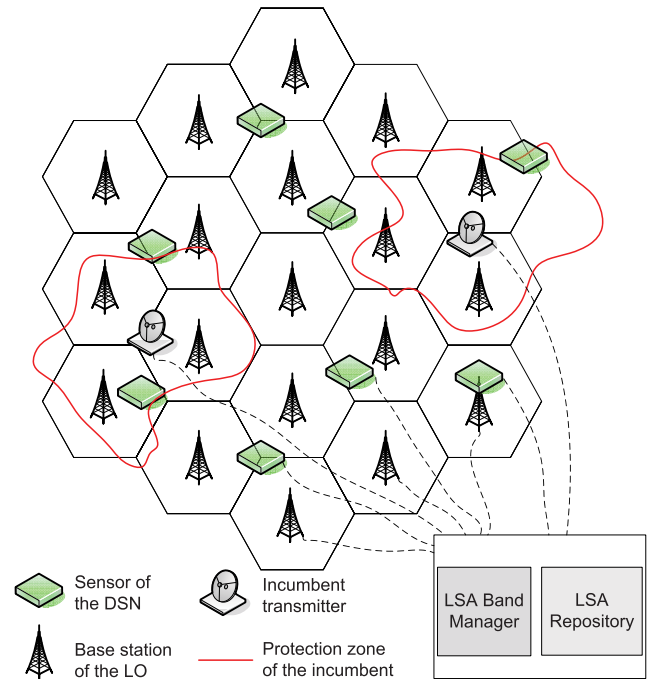
#### A. SYSTEM ARCHITECTURE AND TOPOLOGY

We refer to both IOs and LOs as LSA players, as they both can potentially access the same resources in the available band. Spectrum sharing among LSA players is managed by the central controller (CC). There, several components interact together in order to guarantee that the radio resources are utilized according to the agreed sharing rules.

In the core of this architecture lies the LSA Band Manager (BM), which coordinates the access of incumbents and licensees to the available band. The BM decides on how and to which operator the spectrum is assigned, taking into account: a) the LSA agreements, b) the requirements and demands from incumbents and licensees, and c) information on the current and past usage of the spectrum. The BM is also responsible for enforcing the agreed policies and assigning penalties to misbehaving nodes.

The information on the spectrum usage is retrieved from the LSA repository, which is a database that contains data on the channel availability and history of spectrum usage by incumbents and licensees. In addition, it contains the data on the locations and on the transmit power of each IOs' and LOs' transmitters, as well as their antenna patterns.

The network architecture also includes the DSN that refines the time and spacial granularity of the spectrum usage database in the LSA repository; in addition, it is used for the sensing of any unauthorized transmissions over the LSA bands, thus enabling misbehavior detection of the LOs. More information on the system's architecture can be found in [11]. The topology of our network, including IOs, LOs and the DSN, over a specified geographical area of interest, is depicted in Fig. 1.



**FIGURE 1.** Topology of the proposed network: incumbents and licensees coexist with the DSN, which serves the purpose of monitoring the spectrum. The LOs' base stations, sensors of the DSN, and IOs' transmitters communicate to the LSA Repository and LSA Band Manager, where the latter orchestrates the access to the LSA bands.

#### B. DEDICATED SENSING NETWORK (DSN)

The DSN of our proposed policy enforcement approach is composed of  $N_S$  Radio Frequency (RF) powered antennas, which are randomly distributed over the area of interest aiming at supervising the LO's activity. The DSN serves the purpose of sensing and reporting the data regarding the LOs' spectrum usage to the BM, where such data are further processed for misbehavior detection and penalty enforcement. It should be noted that, even though the sensors are distributed in the network, their operation is coordinated and controlled by the BM, which acts as a central entity for the LSA system.

#### C. RESOURCE SHARING AND POLICY VIOLATION IN LSA

One of the principles that underpins the LSA framework is that both IOs and LOs should have "guaranteed spectrum access and protection against harmful interference" [4]. In other words, spectrum sharing should be orchestrated, by the BM, in such a way that LOs and IOs do not interfere one another, so as to guarantee mutual QoS.

Protection against harmful interference is achieved by making sure orthogonality between LSA players in the spectral, spatial, and temporal domain is maintained.<sup>2</sup> For example, LOs do not have exclusive access to specific LSA channels, but each LSA channel in a given area can be used by several LOs over separate time slots in order to maintain

<sup>2</sup>In every time slot, LSA resource blocks can be thought of as blocks on a 3-dimensional grid, which spans over two spatial dimensions and over frequency.

orthogonality.<sup>3</sup> By allowing LOs to transmit within unused IO resource blocks, the overall system spectral efficiency can be increased.

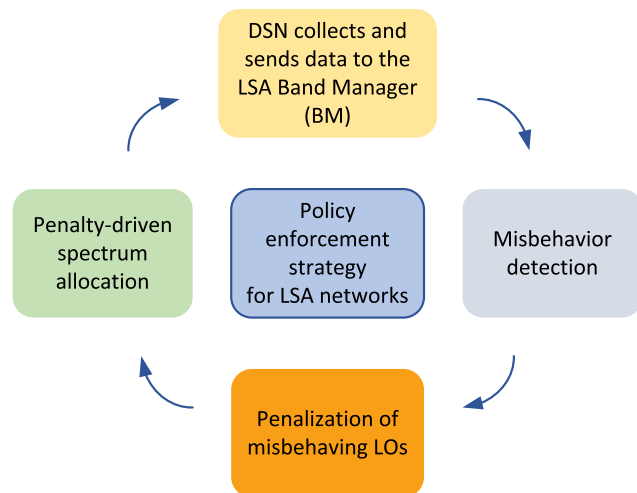
Misbehavior, which we define as an unauthorized transmission over any of the LSA channels, can potentially occur over the temporal, spatial, or spectral domain. Such unauthorized transmissions could be unintentional, e.g., due to faulty hardware, or could be carried out on purpose, to get access to a larger amount of resources than the ones assigned by the BM. In either case, whether intentional or unintentional,<sup>4</sup> spectrum violation leads to harmful interference for the other IOs and LOs, resulting in an inability to guarantee QoS. In general, both IO and LO tiers could attempt to access non-granted resources. However, in this paper, we specifically target the LSA licensees' misbehavior.

#### IV. POLICY ENFORCEMENT APPROACH

The proposed policy enforcement approach consists of three dominant components: i) a misbehavior detection mechanism, which is carried out by the DSN; ii) the penalization of misbehaving users (LOs); and, iii) the allocation of resources based on each operator's penalty. We have particularly focused on the case of LO misbehavior detection during the time slots in which the IOs are active (transmitting). In other words, we do not consider misbehavior among LOs (for example, when IOs are inactive). Our policy enforcement process is depicted in Fig. 2. If LOs do not misbehave, resources are allocated according to a Round-Robin (RR) scheduling [12]. However, any other scheduling policy, or combination of policies, could be used, instead. It should be noted that the novelty of our proposed approach

<sup>3</sup>The non-exclusivity of LSA channels for LOs was proposed in the FP7 Research Project ADEL.

<sup>4</sup>Distinguishing between intentional or unintentional violation of the spectrum usage is not considered in our proposed framework.



**FIGURE 2.** Block diagram demonstrating the steps of the policy enforcement strategy for LSA networks. The procedure requires cooperation between the DSN and the BM: the former carries out sensing and sends the sensing data to the BM; the latter is responsible for misbehavior detection, assigning penalties and allocating the shared spectrum.

lies on the combination of these components for the enhancement of the LSA system, rather than on each individual technique. To the best of our knowledge, this is the first time that such a mechanism is proposed for an LSA network architecture.

#### A. MISBEHAVIOR DETECTION

The data collected from the DSN is transferred to the BM, where a centralized process is initialized. A graphical representation of the misbehavior detection process is depicted in Fig. 3. For the misbehaving activity and its detection, we have assumed the following:

- All the sensors of the DSN monitor the spectrum continuously.
- The licensees misbehave only scarcely, due to the fact that this is an improper activity.<sup>5</sup> Thus, the transmitted signal from the LO's BSs is modeled as a sparse vector (with only a few nonzero locations) and the detection is performed by exploiting the related sparse optimization techniques [13]. In practice, we consider that less than 20% of the LO's BS are potentially misbehaving at any time.
- The channels  $h_{n,k} \in \mathbb{C}$  between the  $n$ -th sensor and the  $k$ -th BS are block fading, frequency flat, and are assumed to be known to the system within a small symbol interval  $T_S$ , as also considered in [14]–[16].
- The signal of the IOs is also received at the DSN's sensors. However, it is assumed that the IOs do not misbehave, and hence, they are excluded from the detection process.<sup>6</sup>

The misbehavior detection process is performed in two phases:

##### a: PHASE ONE

For the misbehavior detection and due to the nature of the task, we have selected a sparse optimization approach.<sup>7</sup> The sparse optimization algorithm operates on the signal and computes an estimate of the transmitted signal, i.e.,  $\hat{x}_k(t)$ . The transmitted signal at time instance  $t$  from the  $k$ -th BS (which belongs to a known LO) is denoted as  $x_k(t) \in \mathbb{C}$ ,  $t = 1, \dots, T_S$ . Since the number of misbehaving (active) licensees,  $N_T$ , is much smaller than the number of all possibly active BSs over the area of interest,  $M$ , the transmission vector containing the signals transmitted from all BSs is modeled as a sparse one, denoted as  $\mathbf{x}_*(t) \in \mathbb{C}^M$ . Moreover, we assume that the status (active/inactive) of the BSs remains unchanged within the sampling period  $T_S$ . Thus, the sparsity level of the transmission vector is guaranteed to be  $\|\mathbf{x}_*(t)\|_0 \leq N_T \ll M$  for all  $t = 1, \dots, T_S$ , where  $N_T$  is the maximum number of LO's active BSs. The signal sample received at each  $n$ -th sensor is assumed to be of the linear form:

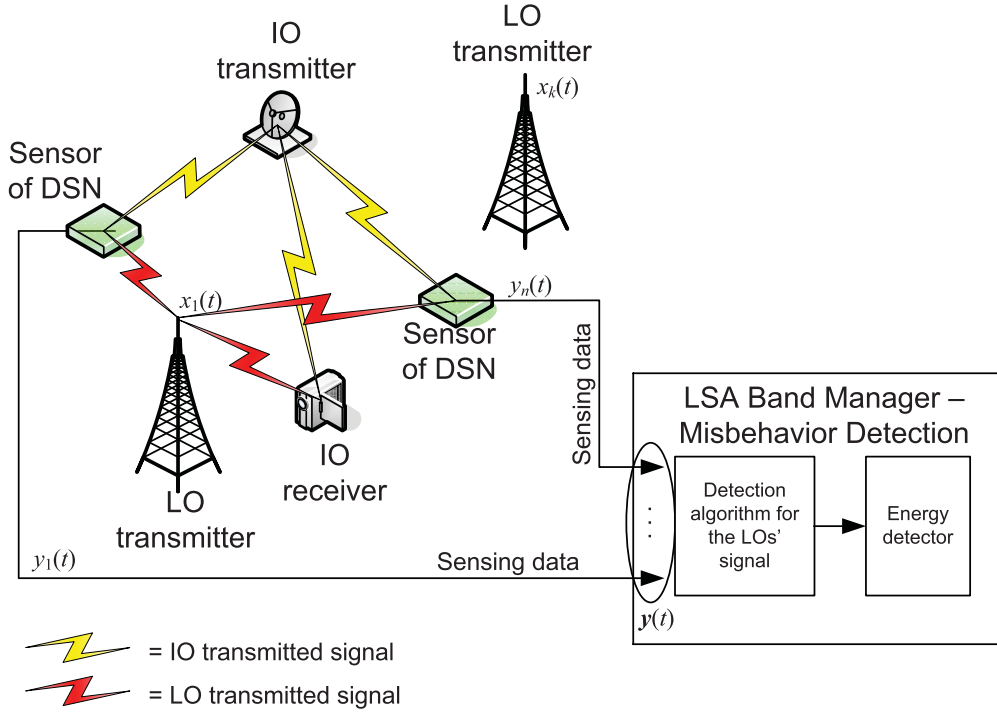
$$y_n(t) = \mathbf{h}_n^H \mathbf{x}_*(t) + v_n(t), \quad n = 1, \dots, N_S, \quad (1)$$

<sup>5</sup>In the sense that it violates the agreed rules.

<sup>6</sup>The location of the IOs' BSs is known.

<sup>7</sup>Other detection schemes may also be applied.





**FIGURE 3.** Misbehavior detection process. The sensors of the DSN first collect the data  $y_n(t)$  and then forward them to the LSA band manager. Next, the detection algorithm performs an estimation of possibly unauthorized transmission. The process is concluded by the classification of the LO's activity (misbehaving or not) according to an energy detection over a small symbol period.

where  $\mathbf{h}_n := [h_{n,1}, \dots, h_{n,M}]^H$  characterizes the channels between the  $n$ -th sensor and all possible  $M$  locations and  $v_n(t)$  is the additive noise assumed i.i.d. with zero mean and bounded variance, uncorrelated with  $h_{n,k}$ . In a more compact form, equation (1) can be cast as:

$$\mathbf{y}(t) = \mathbf{H}\mathbf{x}_*(t) + \mathbf{v}(t), \quad (2)$$

where  $\mathbf{y}(t) = [y_1(t), \dots, y_{N_S}(t)]^T$ ,  $\mathbf{H}^H = [\mathbf{h}_1 \dots \mathbf{h}_{N_S}]$  and  $\mathbf{v}(t) = [v_1(t), \dots, v_{N_S}(t)]^T$ .

For the estimation of the signal,  $\mathbf{x}_*(t)$ , we exploit sparse optimization techniques. Our goal is to solve the following minimization task:

$$\begin{aligned} \min_{\mathbf{x}(t)} \quad & \|\mathbf{x}(t)\|_0 \\ \text{s. t.} \quad & \|\mathbf{y}(t) - \mathbf{H}\mathbf{x}(t)\|_2 \leq \epsilon, \quad \text{for all } t = 1, \dots, T_S. \end{aligned} \quad (3)$$

The cost function in (3) is non-convex and the optimization task is known to be NP-hard [17]. Thus, we will attempt to solve a relaxation of the original task. At each  $t = 1, \dots, T_S$  we solve the Iteratively Reweighted Least Absolute Shrinkage and Selection Operator (IR-LASSO) [18], [19], whose solution is given by:

$$\begin{aligned} \hat{\mathbf{x}}^{(i)}(t) := \arg \min_{\mathbf{x}(t)} \quad & \left\{ \frac{1}{2} \|\mathbf{y}(t) - \mathbf{H}\mathbf{x}(t)\|_2^2 \right. \\ & \left. + \mu \sum_{j=1}^{M^2} w_{jj}^{(i-1)} |x_j(t)| \right\}, \end{aligned} \quad (4)$$

$$w_{jj}^{(i-1)}(t) = \frac{1}{|\hat{x}_j^{(i-1)}(t)| + \epsilon}, \quad i = 1, 2, \dots, \quad (5)$$

where  $\hat{\mathbf{x}}^{(0)}(t)$  is the LASSO solution computed by the Soft-Thresholding with Exact Line search Algorithm (STELA), which was introduced in [14], and  $\epsilon$  is a small threshold that ensures stability. The optimization task attempts to estimate the unknown sparse vector, iteratively. Usually a few iterations over the index  $i$  are sufficient for the convergence of the method. The method is well studied and enjoys better statistical properties compared to the LASSO solution. For the solution of (3) we employ an algorithm that was proposed in [20]. The scheme is known as the Weighted Soft-Thresholding with Exact Line search Algorithm (WSTELA), which was based on a refinement of the STELA. Our proposed detection method attains a high probability of detection and a low probability of false alarm. In addition, the computational cost of this method is significantly reduced, compared to other popular solvers such as the Alternating Direction Method of Multipliers (ADMM) [21]. More details on the algorithm and its performance in terms of detection can be found in [20].

#### b: PHASE TWO

An energy detector operates on the estimated signal and the activity of the LO is classified as non-misbehaving- $\mathcal{H}_0$  or misbehaving- $\mathcal{H}_1$ . In order to successfully detect (by correctly classifying) an unauthorized transmission from an LO the system should: i) recover the support of the sparse vector  $\mathbf{x}_*(t)$  (which reveals the location of the transmitters)

and ii) compute a good estimate of the transmitted signal's values. Instead of applying a standard thresholding technique on the transmitted signal, we perform an energy detection<sup>8</sup> on the estimated signal,  $\hat{x}(t)$ , over a small symbol period,  $T_S$ :

$$E_k = \frac{1}{T_S} \sum_{t=1}^{T_S} |\hat{x}_k(t)|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\geq}} \tau_{ed}(k), \quad (6)$$

where  $\tau_{ed}(k)$  is a model-defined threshold depending on the agreed power transmission levels for each LO. In the simplest scenario, where no transmissions are authorized by the IO's network,  $\tau_{ed}(k)$  is set at the noise level for all LOs. For those BSs that are allowed to transmit, the threshold is set at the power level allocated by the BM. Since the locations of the BSs and the channels between each BS and DSN sensor are known to the LSA BM, and due to the unique mapping between BSs' indices and LOs, the misbehaving LOs can be directly identified from the respective indices. The detection results, i.e., indices  $k$  such that  $E_k > \tau_{ed}(k)$ , and the probabilities of detection and false alarm are then used for determining the severity of the agreement violation and assigning the penalty.

*Remark 1:* Another strong advantage of using sparse modelling techniques with respect to non-sparse ones relates to the size of the DSN. The signal can be detected with fewer observations,  $N_S$ , than the size,  $M$ , of the unknown vector, i.e.,  $\mathbf{x}_*(t)$ ,  $t = 1, \dots, T_S$ . Thus, it is possible to reduce the number of required sensors, and, in such way, provide cost benefits as well. However, more sensors lead to better detection results; the probabilities of detection,  $P_d$ , and false alarm,  $P_{fa}$ , depend on the number of sensors that are used for the detection. Hence, there is a clear tradeoff between the implementation cost of the DSN and the accuracy of the estimation that we would like to achieve.

### B. PENALIZATION OF THE MISBEHAVING LOS

Whenever an LO is detected to misbehave (classified as  $\mathcal{H}_1$ ) a maximum penalty  $A_{max}$  is applied. Since the probabilities of detection and false alarm depend on the number of sensors that are used for the detection, we scale the value of the penalty according to the confidence level of the misbehavior detection. Therefore, we set  $A = (\bar{P}_d - \bar{P}_{fa})A_{max}$ , where  $\bar{P}_d$  is the average probability of successful detection and  $\bar{P}_{fa}$  is the average probability of false alarm. Once applied, the penalty value reduces over time, following an exponential decay, as long as the penalized LO does not misbehave again, according to:

$$P_k^n = Ae^{-(t-t_{kn})/\lambda}, \quad (7)$$

where  $t$  is the current time,  $t_{kn}$  is the time at which the previous misbehavior was detected,  $\lambda$  is the half-life time constant which determines how quickly the penalty decays. However, if subsequent violations of the sharing rules are detected, additional penalties are assigned and added to the

current penalty value of the detected LO. Finally, it should be noted that the average probabilities of detection and false alarm also depend on the number of transmitting BSs.

### C. PENALTY-DRIVEN RESOURCE ALLOCATION

At the final stage of our policy enforcement strategy, we allocate resources to the LO with the lowest penalty value, if their values are below a predefined threshold. For operators that have equal penalties, the allocation is performed according to Round-Robin scheduling. If an operator's penalty value, given by (7), is above the threshold, it is excluded from the sharing process; in other words, only LOs below the defined threshold compete for the available resources. On the other hand, if all players have penalty values above the threshold, the resources remain unallocated.<sup>9</sup> Hence, our enforcement strategy not only punishes misbehavior but also rewards compliance to the agreed rules.

### V. LSA SYSTEM-LEVEL SIMULATOR SETUP

Compared to existing system-level simulators, such as the Vienna LTE System Level Simulator (SLS) [22], our simulator shifts the focus towards the components of the LSA paradigm that are typically absent. The proposed LSA setup includes the IOs, Mobile Network Operators (MNOs) for the role of LOs, an LSA repository and the BM, as well as a DSN. In the following, we describe the system blocks and the models implemented in the LSA simulator and that are functional to our investigation.

#### A. BLOCK FEATURES IN THE PROPOSED LSA SYSTEM SETUP

In the simulator, we have implemented the following features of the LSA system blocks.

#### C: FUNCTIONALITIES OF THE LSA BAND MANAGER

- **Allocation of the available LSA channels to IOs and MNOs.** Several LSA players can request spectrum, which is scarce and needs to be allocated in order to serve the demand and prevent interference. Scheduling takes into account the spectrum availability, the request for access by incumbents and MNOs, the previous usage of spectrum, and possible misbehavior of the MNOs.
- **Determining and granting access to the set of BS cells that an MNO can use.** Access to spectrum is granted on a geographical basis, i.e., MNOs that are granted resources will be allowed to use only the BSs that are far enough from the active BSs of IOs in order to prevent interference. In addition, only some sectors of a BS might be activated. The BM undertakes the task of determining which BSs and which sectors can be used by the MNOs. The goal is to ensure that the IOs experience a satisfactory signal quality.
- **Applying policy enforcement.** The BM is responsible for the detection of potential misbehavior and application of a penalty, e.g., by restricting access to

<sup>8</sup>Other methods could also be applied, however, we chose the energy detector due to its robustness.

<sup>9</sup>This does not extend to the Incumbent Operator, which preserves its right to access the spectrum regardless of the behavior of the LOs.

spectrum for those players that are found to misbehave. The penalty attributed to each MNO is applied during the scheduling procedure, prioritizing MNOs with lower, or zero, penalty.

#### d: LSA REPOSITORY

The repository keeps logs of all the spectrum activities occurring in the LSA band and, in particular, records of current geographical usage of every channel for each operator. In addition, it contains the data on the location of the transmitters, the transmit power, and the antenna radiation patterns. All this information is utilized so that we can estimate the potential interference generated by transmitters on unintended receivers. The LSA repository is accessed by the LSA BM. The data required to build the database are retrieved from the spectrum users (incumbents and licensees).

#### e: DEDICATED SENSING NETWORK (DSN)

The DSN of our proposed policy enforcement approach is composed of 50 sensors, which are randomly distributed over the area of interest where MNO's BSs are deployed. For the detection cycle we have used a value of  $T_S = 10$  symbols.

### B. SYSTEM-LEVEL SIMULATOR ARCHITECTURE

In this section, we describe the modules of the system-level simulator and how they interact with one another. A graphical representation of the proposed simulator architecture is provided in Fig. 4.

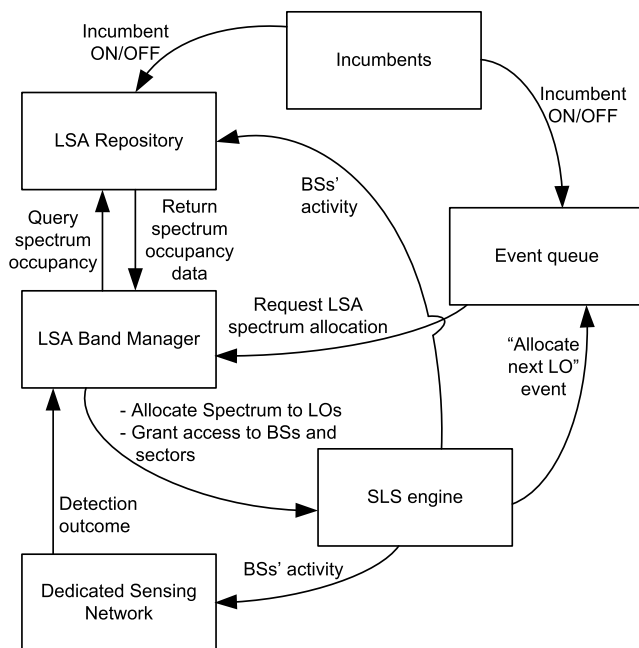


FIGURE 4. Modules of the LSA system-level simulator and their interfaces.

As observed from Fig. 4, the functioning of the simulator is triggered by an *event queue*, which keeps records of the different modules' activities and operates as a timer for the LSA BM (which also sets the timer for the entire simulator).

The possible events that are logged in the queue are: (i) the incumbent activation; and (ii) the allocation of the next LO on the LSA band. The former event is generated by the *incumbent* module — which implements the IOs and generates their activity, i.e., it switches them on and off. The latter event occurs when the allocation period of the LO on the LSA band is over and another LO needs to be allocated on this band.

The *LSA Band Manager module* is triggered by the event queue and allocates the LSA spectrum to the LOs. In addition, the LSA BM grants LOs access to the LSA spectrum on a sector-basis. The data regarding spectrum occupancy can be fetched from the *LSA Repository module*, which stores the information on the IO and LO activity over the LSA spectrum. It should be noted that this allocation takes into account the current availability of the spectrum (which depends on the IOs' activity), its past usage and the policy enforcement penalty.

Whenever the LSA BM block schedules an LO, the *System-Level Simulator (SLS) engine module* produces the results in terms of throughput, band occupancy and misbehavior of the LOs. Finally, the *Dedicated Sensing Network module* retrieves data regarding the BSs' activity from the SLS engine block and performs the misbehavior detection; the outcome of this process is then fed to the LSA BM for policy enforcement purposes.

### C. NETWORK LAYOUT

As a specific application for the incumbent, we assume a system for video surveillance.<sup>10</sup> In the simulator, we model each IO as a transmitter and a set of 10 receivers uniformly distributed over a circular area, which we call *protection zone*. This zone is the area within which the incumbent receivers should be guaranteed a given signal quality. The incumbent transmitters, which transmit on a given channel and all with the same fixed power, can either transmit or remain in a stand-by (or idle) state: the ratio of the IOs' activity is defined by its duty cycle. With reference to Fig. 4, the modeled IO is implemented in the incumbent module.

The LOs are implemented in the SLS engine module (see Fig. 4). We assume that each MNO transmits over an exclusively licensed band and over a 5MHz LSA channel, which is shared between the IOs and several MNOs. We assume that two MNOs operate in the same band, where, up to five IOs—distributed across the network—can be active.

The LSA MNOs (licensees) are modelled as three-sector macro-sites, whose BSs are deployed in a hexagonal grid. We consider a scenario of 19 sites, arranged in three concentric rings. Each sector is served by a directional antenna and the transmit power is 43dBm per LSA channel [23].

We model the signal propagation with Extended Hata model and Rayleigh small-scale fading. In order to limit the computational complexity associated with the physical

<sup>10</sup>The LSA framework includes several and various types of users of the LSA band, which range from military services, radar systems, amateur radio users, and wireless cameras, etc. [4].

layer (PHY), we assume a given cell spectral efficiency value, i.e., whenever a cell is active, its cell spectral efficiency is constant.

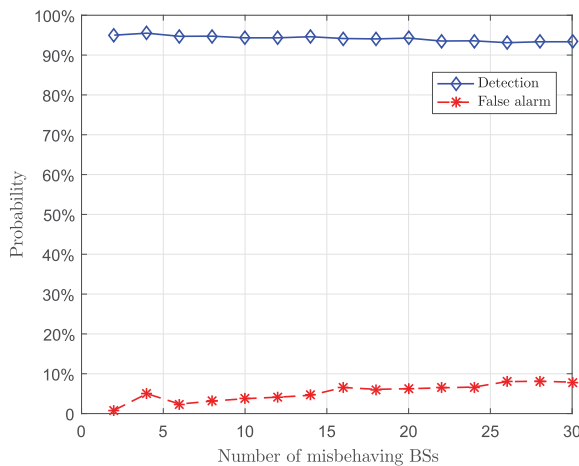
## VI. SYSTEM-LEVEL RESULTS

In this section, we present our results from system-level simulations using the proposed policy enforcement mechanism for an LSA network. The values of the main parameters used for the simulation results are reported in Table 1.

**TABLE 1. Simulation parameters.**

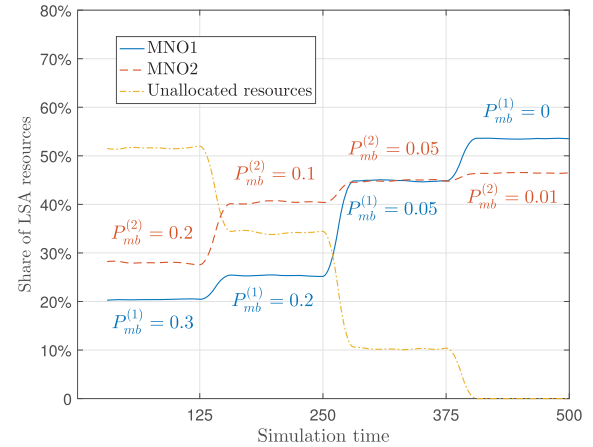
Parameter	Value
Incumbent duty-cycle	10%
Number of IUs	5
Number of receivers per incumbent transmitter	10
Incumbent TX power	20dBm over 20MHz, corresponding to 14dBm over 5MHz
Incumbent radius	50m
LSA licensees BS	43dBm TX power per sector, serving a three-sector site with directional antennas
Sites	19 per operator (3 sectors each site)
MNOs	2
MNO cell spectral efficiency	2.23bps/Hz [23, See 2x2 SU-MIMO Rel. 8 - FDD in 3GPP - Tables 10.1.1.1-1, 10.1.1.2-1]
Sensors of DNS	50

First, we compute and present the average probabilities of detection and false alarm for several misbehaving BSs. Next, we present the allocation of resources according to our policy enforcement approach. Finally, we depict the sensitivity of the penalty threshold on the allocation of resources.



**FIGURE 5. Average probabilities of detection and false alarm, while varying the number of LO's misbehaving BSs.**

Fig. 5 shows the probabilities of detection and false alarm for the proposed detection algorithm, i.e., the WSTELA solver for the IR-LASSO task, while we vary the number of misbehaving BSs. Our method achieves successful detection with probability above 90% for up to 30 misbehaving BSs out of a total of 57 BSs, while it keeps the probability of false alarm below 10%. It should be noted that for the regularization parameter  $\mu$  in (4) we have used the cross-validation



**FIGURE 6. Change of LSA resource share over time due to changes in the behavior of the two MNOs. The probability for MNO1 is  $P_{mb}^{(1)}$  and for MNO2 is  $P_{mb}^{(2)}$  and changes every 125 simulation steps.**

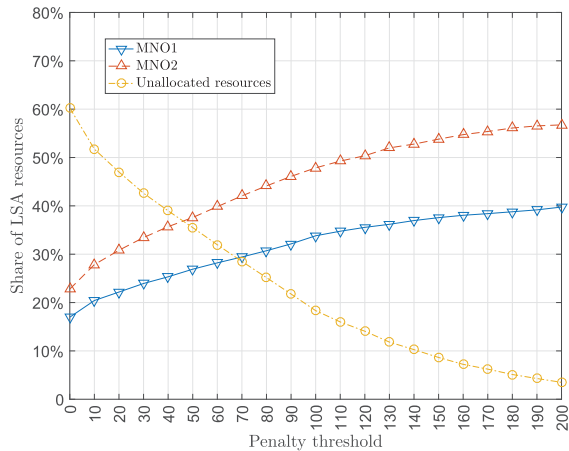
technique in order to find the best values for both algorithms STELA and WSTELA.

As discussed in Section V-C, the BM may choose to block the allocation of resources for operators whose penalty score exceeds a certain threshold value. If all operators' scores exceed the defined threshold, the LSA resources would remain unallocated. While this approach leads to an under-utilisation of the available LSA resources, it strengthens the incentives for MNOs to comply with the LSA rules.

Fig. 6 shows the allocation of resources to two competing MNOs over time due to variations on their behavior. The probability of misbehaving, i.e.,  $P_{mb}^{(i)}$ ,  $i = 1, 2$ , for the two operators varies every 125 simulation steps as follows: for MNO1  $P_{mb}^{(1)}$  changes from 0.3 in the first 125 steps, to 0.2, then 0.05 and finally 0 (i.e. full compliance with the LSA rules); for MNO2 the  $P_{mb}^{(2)}$  changes from 0.2 to 0.1, then 0.05, and finally 0.01. The penalty threshold during this simulation was set to 10. Our policy enforcement algorithm always benefits the MNO that complies more with the LSA rules. We emphasize to the fact that misbehavior does not lead to complete exclusion from the LSA resources. However, the share of the resources allocated to each misbehaving MNO is such that, even if misbehavior led to short-term gains (from unauthorized transmissions), the MNO would encounter a significant loss over the allocated resources on the long-term compared to being under full compliance with the agreed rules. In the case where MNO1 fully complies with the rules while MNO2 misbehaves with probability 0.01 (time period 375 to 500 in Fig. 6), the allocation algorithm makes sure that all the available resources are fully utilised, while the complying MNO is further rewarded for its behavior. Similarly, when both MNOs misbehave with the same probability (0.05), they both receive equal share of the available resources, but approximately 10% of the LSA resources remain unallocated by the BM.

The level of the penalty threshold is key to policy making. Fig. 7 shows the average allocation of resources to two





**FIGURE 7.** Changing the penalty threshold further penalizes misbehaving MNOs but can lead to lower utilization of available LSA resources.

MNOs who misbehave with probability 0.3 for MNO1 and 0.2 for MNO2, for different values of the penalty threshold. The same figure shows the share of resources that remain unallocated for the defined threshold. It is observed that, lower values of the penalty threshold lead to MNOs being severely penalised for not adhering to the LSA rules. With lower values of the threshold then each MNO has incentives to comply with the LSA rules, regardless of what other MNOs do. This is attributed to the fact that by increasing its own level of compliance it gains access to a larger amount of resources that would otherwise remain unallocated. At the same time, however, a lower threshold may lead to the LSA resources being underutilised. On the other hand, higher values of the threshold lead to “competitive” incentives where each MNO has incentives to misbehave less than other MNOs sharing the same resources. As depicted in Fig. 7, it is observed that, higher threshold values lead to better utilization of the LSA resources; however, lower thresholds create a better set of incentives against misbehavior from the licensees, which leads to better overall policy outcomes.

## VII. CONCLUSION

In this paper, a policy enforcement strategy for LSA is presented. In order to guarantee the reliability of the system and moreover provide QoS to its users, we propose a policy enforcement mechanism that is built within the sharing network architecture. The general concept is to penalize misbehaving activity from the licensees based on spectrum sensing information provided by a Dedicated Sensing Network (DSN).

The three key components on which the proposed policy enforcement strategy is built on are: a) the DSN and a misbehavior detection algorithm, attaining low probabilities of misdetection and false alarm (below 10%), b) a penalization function that calculates a penalty score for each LO, and, c) a resource allocation algorithm that allocates the shared resources taking into account the penalty scores of the licensees. To the best of our knowledge, this is the first time that such a mechanism is proposed in LSA networks.

Furthermore, we provide an open source simulation tool for spectrum sharing in LSA networks, which performs the entire policy enforcement procedure.

Through our system-level results we demonstrate that: a) misbehaving occurrences can be successfully detected by our proposed mechanism, b) the allocation of resources can change from the static model of equal allocation to both misbehaving and non-misbehaving LOs to a more dynamic one that takes penalty scores into account and c) the severity of the penalty can be centrally controlled (thus it is fair for all operators) by the central controller.

We recognize that cases of severe misbehavior may require regulatory intervention, including financial penalties and license revoking—an approach that is currently followed by NRAs for illegal transmissions and harmful interference management. However, regulatory intervention is typically time-consuming and incurs significant costs to the NRA. Our proposed solution provides distinct advantages over the existing mechanisms because of its near real time response and shifting of responsibility of misbehavior detection to the industry as well. We believe that our policy enforcement strategy could unlock the deployment of spectrum sharing architectures, such as LSA, for next generation wireless systems.

## ACKNOWLEDGEMENT

Dr. K. Voulgaris carried out this research work while at Athens Information Technology. At the time of this publication he has moved to the European Investment Bank as a technical expert within the JASPERS department.

## REFERENCES

- [1] J. Mitola and G. Q. Maguire, “Cognitive radio: Making software radios more personal,” *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.
- [2] J. Mitola, “Cognitive radio—An integrated agent architecture for software defined radio,” Ph.D. dissertation, Roy. Inst. Technol., Stockholm, Sweden, May 2000. [Online]. Available: [https://web.archive.org/web/20120917062752/web.it.kth.se/~maguire/jmitola/Mitola\\_Dissertation8\\_Integrated.pdf](https://web.archive.org/web/20120917062752/web.it.kth.se/~maguire/jmitola/Mitola_Dissertation8_Integrated.pdf)
- [3] M. D. Mueck, S. Srikanteswara, and B. Badic, “Spectrum sharing: Licensed shared access (LSA) and spectrum access system (SAS),” Intel, Tech. Rep. Version 1.0, Oct. 2015. [Online]. Available: <https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/spectrum-sharing-lsa-sas-paper.pdf>
- [4] European Conference of Postal and Telecommunications Administrations (CEPT), “ECC report 205—Licensed shared access (LSA),” Tech. Rep., Feb. 2014. [Online]. Available: <http://www.ero.docdb.dk/Docs/doc98/official/pdf/ECCREP205.PDF>
- [5] *Code for the System Level Simulator for Policy Enforcement in LSA-Enabled Networks*. Accessed: Nov. 2017. [Online]. Available: [https://github.com/g-carlo/LSA\\_pol\\_enforcement\\_SysSim](https://github.com/g-carlo/LSA_pol_enforcement_SysSim)
- [6] M. Maruenda-Hernández, F. Pérez-González, and S. K. Jayaweera, “A subspace-based policy enforcement method in dynamic spectrum leasing schemes,” in *Proc. IEEE 13th Int. Conf. Commun. Technol. (ICCT)*, Sep. 2011, pp. 1118–1123.
- [7] V. Kumar, J.-M. J. Park, and K. Bian, “PHY-layer authentication using duobinary signaling for spectrum enforcement,” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 1027–1038, May 2016.
- [8] A. Dutta and M. Chiang, “‘See something, say something’ crowdsourced enforcement of spectrum policies,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 67–80, Jan. 2016.
- [9] M. B. H. Weiss, W. Lehr, M. Altamimi, and L. Cui, “Enforcement in dynamic spectrum access systems,” in *Proc. TRPC Conf.*, Mar. 2012.

- [10] M. M. Butt, C. Galiotto, and N. Marchetti, "Fair and regulated spectrum allocation in licensed shared access networks," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–6.
- [11] A. Morgado et al., "Project deliverable D3.1: Reference scenarios, network architecture, system and user requirements and business models," FP7 Research Project ADEL-No: 619647, Dec. 2014, accessed: Dec. 2017. [Online]. Available: <http://www.fp7-adel.eu/deliverables.html>
- [12] L. Kleinrock, "Analysis of a time-shared processor," *Naval Res. Logistics*, vol. 11, no. 1, pp. 59–73, 1964.
- [13] A. M. Bruckstein, D. L. Donoho, and M. Elad, "From sparse solutions of systems of equations to sparse modeling of signals and images," *SIAM Rev.*, vol. 51, no. 1, pp. 34–81, 2009.
- [14] Y. Yang and M. Pesavento, "A novel line search method for non-smooth optimization problems," in *Proc. IEEE 23rd Eur. Signal Process. Conf. (EUSIPCO)*, Aug./Sep. 2015, pp. 1726–1730.
- [15] Y. Yang, M. Zhang, M. Pesavento, and D. P. Palomar, "An online parallel algorithm for spectrum sensing in cognitive radio networks," in *Proc. IEEE 48th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2014, pp. 1801–1805.
- [16] S.-J. Kim and G. B. Giannakis, "Optimal resource allocation for MIMO ad hoc cognitive radio networks," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3117–3131, May 2011.
- [17] S. Theodoridis, *Machine Learning: A Bayesian and Optimization Perspective*. San Francisco, CA, USA: Academic, 2015.
- [18] R. Tibshirani, "Regression shrinkage and selection via the lasso," *J. Roy. Stat. Soc. B, Methodol.*, vol. 58, no. 1, pp. 267–288, 1996.
- [19] B. A. Johnson, Q. Long, Y. Huang, K. Chansky, and M. Redman, "Model selection and inference for censored lifetime medical expenditures," *Biometrics*, vol. 72, no. 3, pp. 731–741, 2016.
- [20] G. Papageorgiou, K. Voulgaris, and C. Papadias, "Sparse modeling methods for misbehavior detection in LSA networks," in *Proc. Global Wireless Summit (GWS)*, 2016.
- [21] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Found. Trends Mach. Learn.*, vol. 3, no. 1, pp. 1–122, Jan. 2011.
- [22] M. Rupp, S. Schwarz, and M. Taranetz, *The Vienna LTE-Advanced Simulators*. Singapore: Springer-Verlag, 2016.
- [23] *Further Advancements for EUTRA Physical Layer Aspects (Release 9)*, document 3GPP TR 36.814 V9.0.0 (2010-03), 3GPP, Mar. 2010.



**CARLO GALIOTTO** received the M.Sc. degree in telecommunications engineering from the University of Padova, Italy, in 2009, and the Ph.D. degree in electronic and electrical engineering from the CONNECT-Centre for Future Networks and Communications, Trinity College Dublin, Ireland, in 2017. He spent over two years as a Researcher with Aalborg University, Denmark, from 2009 to 2011, where he was involved in passive RFID systems and on radio resource management for heterogeneous cellular networks. His current research interests include the study of performance and issues of extremely dense networks and small cells, and spectrum sharing for 5G systems.



**GEORGE K. PAPAGEORGIOU** received the M.Sc. degree in applied mathematics and the Ph.D. degree in signal processing from the National and Kapodistrian University of Athens, Greece, in 2012 and 2016, respectively. From 2007 to 2015, he was teaching mathematics in several educational institutions. Since 2016, he has been a Researcher with the Broadband Wireless and Sensor Networks Laboratory, Athens Information Technology. He has been involved in several European funded projects (ADEL, SANSA, and 5G blueSPACE), as well as several industrial projects. His research activities include signal processing with applications to wireless networks, compressed sensing, adaptive filtering, distributed networks, mathematical modeling and optimization, nonlinear approximation, and information theory. He has participated in over-the-air demos, one of which received the Best Booth Award at the EuCNC 2016 Conference in Athens (FP7 Project ADEL).



**KONSTANTINOS VOULGARIS (M'17)** received the B.Sc. degree in physics from the University of Patras in 1999, the M.Sc. degree in computers, communications and human centred systems from the University of Birmingham in 2000, and the Ph.D. degree in telecommunications research from the University of London-King's College in 2009. He has over 15 years of professional experience across engineering, research, and regulatory policy-making roles in sector-leading organisations including Motorola, T-mobile, Bell Labs, and Ofcom. He has participated in multiple FP-6, FP-7, and H2020 EU-funded research projects in the areas of IoT, spectrum sharing, and satellite communications. His interests lie in the research areas of radio resource allocation and cross-layer interactions in wireless communications systems, as well as technology innovation and strategic policy making.



**M. MAJID BUTT (SM'15)** received the M.S. degree in telecommunication from Christian Albrechts University, Kiel, Germany, and the Ph.D. degree from the Norwegian University of Science and Technology, Norway. He has held Senior Researcher positions at Trinity College Dublin, Ireland, and Qatar University. He is currently an Assistant Professor with the University of Glasgow, U.K. He held European research consortium for informatics and mathematics (ERCIM) Post-doctoral Fellow positions at Fraunhofer Heinrich Hertz Institute, Germany, and the University of Luxembourg. His major areas of research interest include communication techniques for wireless networks with particular focus on radio resource allocation, scheduling algorithms, cooperative communications, cross-layer design, energy harvesting, and green communication techniques. He has authored over 40 peer reviewed conferences and journal publications in these areas. He was a recipient of the Marie Curie Alain Bensoussan Post-Doctoral Fellowship from ERCIM. He has been an Associate Editor for the IEEE Access and the IEEE Communication Magazine since 2016.



**NICOLA MARCHETTI** received the Ph.D. degree in wireless communications from Aalborg University, Denmark, in 2007, the M.Sc. degree in electronic engineering from the University of Ferrara, Italy, in 2003, and the M.Sc. degree in mathematics from Aalborg University in 2010. He is currently an Assistant Professor in wireless communications with Trinity College Dublin, Ireland. He performs his research under the Trinity Information and Complexity Labs and the Irish Research Centre for Future Networks and Communications. His collaborations include research projects in cooperation with Nokia Bell Labs and U.S. Air Force Office of Scientific Research, among others. His research interests include adaptive and self-organizing networks, complex systems science for communication networks, PHY layer, and radio resource management. He has authored over 100 journals and conference papers, two books, and seven book chapters. He holds two patents. He received four Best Paper Awards.



**CONSTANTINOS B. PAPADIAS** (F'13) received the Diploma degree in electrical engineering from the National Technical University of Athens in 1991 and the Ph.D. degree (Hons.) in signal processing from the Ecole Nationale Supérieure des Télécommunications, Paris, France, in 1995. He was a Researcher with Institut Eurécom from 1992 to 1995, Stanford University from 1995 to 1997, and Bell Labs (as a member of Technical Staff from 1997 to 2001 and as a Technical Manager from 2001 to 2006). He was also an Adjunct Professor with Columbia University from 2004 to 2005 and Carnegie Mellon University from 2006 to 2011. He is currently the Scientific Director of Athens Information Technology, Athens, Greece, where he is also the Head of the Broadband Wireless and Sensor Networks Research Group. He is also an Adjunct Professor with Aalborg University. He has acted as a Technical Coordinator in several EU projects such as: CROWN in the area of cognitive radio; HIATUS in the area of interference alignment; HARP in the area of remote radio heads; and ADEL in the area of licensed shared access. He has published over 190 papers and three books. He has also made standards contributions

and holds 12 patents. He was a member of the Steering Board of the Wireless World Research Forum from 2002 to 2006, a member and an industrial liaison of the IEEE Signal Processing for Communications Technical Committee from 2003 to 2008, and a National Representative of Greece to the European Research Council's IDEAS Program from 2007 to 2008. He has served as a member of the IEEE Communications Society's Fellow Evaluation and Awards Committees and an Associate Editor for various journals. He has contributed to the organization of several conferences, such as the IEEE GLOBECOM 2014 (Workshops Chair), the IEEE CTW 2016 (General Chair), the IEEE ICC 2017 (Workshops Chair), and the upcoming IEEE SPAWC 2018 (General Chair). His distinctions include the Bell Labs President's Award in 2002, the IEEE Signal Processing Society's Young Author Best Paper Award in 2003, the Bell Labs Teamwork Award in 2004, his recognition as a Highly Cited Greek Scientist in 2011, the two IEEE conference paper awards in 2013 and 2014, and the Best Booth Award at EUCNC in 2016. He was a Distinguished Lecturer of the IEEE Communications Society from 2012 to 2013. He has received over 7500 citations for his work, with an h-index of 40.

• • •